目次

はじめに

このたびは弊社の FMV パソコン（以降、パソコン本体）をご購入いただき、まことにありがとうございます。
本書は、パソコン本体に搭載されているセキュリティチップ（以降、本製品）の基本的な取り扱い、セキュリティチップを利用するためのソフトウェアのインストール、およびアプリケーションの設定と使い方について説明しています。
ご使用になる前に本書およびパソコン本体のマニュアルをよくお読みになり、正しい取り扱いをされますようお願いいたします。

2004 年 10 月

■セキュリティ機能について

セキュリティ機能は完全な認証照合、データやハードウェアの保護を保証するものではありません。当社は、お客様がセキュリティ機能を使用されたこと、または使用できなかったことによって生じるいかなる損害に関しても、一切の責任を負いかねますのであらかじめご了承ください。

本書の表記

本文中に記載されている記号には、次のような意味があります。

記号	意味
重要	お使いになる際の注意点や、してはいけないことを記述しています。必ずお読みください。
POINT	操作に関連することを記述しています。必要に応じてお読みください。
→	参照ページや参照マニュアルを示しています。

■コマンド入力（キー入力）

CD-ROM ドライブのドライブ名を、［CD-ROM ドライブ］で表記しています。入力の際は、お使いの環境に合わせて、ドライブ名を入力してください。
例：[CD-ROM ドライブ]：¥setup.exe

■連続する操作の表記

本文中の操作手順において、連続する操作手順を、「→」でつなげて記述しています。

例：　「スタート」ボタンをクリックし、「プログラム」をポイントし、「アクセサリ」をクリックする操作

↓

「スタート」ボタン→「プログラム」→「アクセサリ」の順にクリックします。

また、本文中の操作手順において、操作手順の類似しているものは、あわせて記述しています。

例：　「スタート」ボタン→「(すべての）プログラム」→「アクセサリ」の順にクリックします。

■画面例およびイラストについて

表記されている画面およびイラストは一例です。お使いの機種やモデルによって、実際に表示される画面やイラスト、およびファイル名などが異なることがあります。また、このマニュアルに表記されているイラストは説明の都合上、本来接続されているケーブル類を省略していることがあります。

■製品の呼び方

本文中の製品名称を、次のように略して表記します。
なお、本書ではお使いの機種、または OS 以外の情報もありますが、ご了承ください。

<table>
<tr><th>製品名称</th><th colspan="3">本文中の表記</th></tr>
<tr><td>FMV-E635</td><td>E635</td><td colspan="2" rowspan="7">本パソコン
パソコン本体</td></tr>
<tr><td>FMV-E630</td><td>E630</td></tr>
<tr><td>FMV-K630</td><td>K630</td></tr>
<tr><td>FMV-830NA/H</td><td>NA/H</td></tr>
<tr><td>FMV-830NA/L</td><td>NA/L</td></tr>
<tr><td>FMV-830MG/H</td><td>MG/H</td></tr>
<tr><td>FMV-830MT</td><td>MT</td></tr>
<tr><td>Microsoft® Windows® XP Professional</td><td>Windows XP Professional</td><td rowspan="2">Windows XP</td><td rowspan="3">Windows 注</td></tr>
<tr><td>Microsoft® Windows® XP Home Edition</td><td>Windows XP Home Edition</td></tr>
<tr><td>Microsoft® Windows® 2000 Professional</td><td colspan="2">Windows 2000</td></tr>
<tr><td>Microsoft® Internet Explorer</td><td colspan="3">Internet Explorer</td></tr>
<tr><td>Microsoft® Word</td><td colspan="3">Word</td></tr>
<tr><td>Microsoft® Outlook®</td><td colspan="3">Outlook</td></tr>
<tr><td>Microsoft® Outlook® Express</td><td colspan="3">Outlook Express</td></tr>
<tr><td>Netscape® または Netscape® Communicator</td><td colspan="3">Netscape</td></tr>
</table>

注：Windows XP/2000 のように併記する場合があります。

商標および著作権について

Microsoft、Windows は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
Netscapeは､米国およびその他の国におけるNetscape Communications Corporation社の登録商標です。
その他の各製品名は、各社の商標、または登録商標です。
その他の各製品は、各社の著作物です。

画面の使用に際して米国 Microsoft Corporation の許諾を得ています。

使用上のご注意

■ セキュリティチップで利用する鍵や証明書、パスワードの管理について

セキュリティチップは、複数の鍵や証明書を扱います。これらの鍵や証明書を紛失した場合は、その鍵によって暗号化されたファイル等は読めなくなることがありますので注意してください。またこれらの鍵を利用する際にはパスワードが必要です。パスワードが正しく入力されない場合、鍵が利用できないため紛失時同様その鍵によって暗号化されたファイル等は読めなくなります。

■ セキュリティチップ利用についてのご注意

・本製品で使用するユーティリティおよびアプリケーションをインストールするときには、パソコン本体またはネットワーク上のパソコンに、CD-ROM ドライブが搭載／接続されている必要があります。
・セキュリティチップで鍵を生成する場合、数分かかることがあります。
・Infineon Security Platform ユーティリティについては、Infineon Security Platform ユーティリティのマニュアルを参照してください。
・SMARTACCESS/Trust アプリケーションについては、SMARTACCESS/Trust アプリケーションのマニュアルを参照してください。

・パソコン本体の修理・保守を依頼する場合は、Trusted ログオンを解除してください。
Trusted ログオンを解除していない場合、修理・保守ができないことがあります。Trusted ログオンを解除するには、以下の手順を行ってください。
1.「スタート」ボタン→「(すべての）プログラム」→「SMARTACCESS Trust」→「ログオン設定ツール」の順にクリックします。
「ログオン設定ツール」が表示されます。
2.「ログオン方法変更」をクリックします。
3.「Trusted ログオン」の「使用する」のチェックを外し、「OK」をクリックします。
・パソコン本体の修理・保守が行われた場合には、セキュリティ機能が解除されていることがあります。その場合には環境の再構築が必要となります。詳しくは次の記載を参照してください。
「セキュリティチップ破損等によるパソコン修理後の作業について」（→ P.29）
「パソコン廃却時のセキュリティチップへの設定」（→ P.35）

1 概要

■ セキュリティチップとは

セキュリティチップは、TCG 注 1 の仕様に基づいた TPM 注 2 と呼ばれる IC チップです。TCG により、個人の権利やプライバシーを保護し、かつ様々なセキュリティを実現することができます。セキュリティチップは、TCG セキュリティの基本機能を提供します。セキュリティチップを搭載したパソコンは、ソフトウェアによる攻撃および物理的な攻撃からデータを保護し、より強固なセキュリティを実現します。

注 1：TCG は Trusted Computing Group の略称です。
TCG は、信頼性と安全性を持った新しいコンピュータをつくるためのオープンな業界仕様を策定する団体です。
（https://www.trustedcomputinggroup.org/）

注 2：TPM は Trusted Platform Module の略称です。

■ セキュリティチップの機能

セキュリティチップには、セキュリティチップの管理を行う [所有者] とセキュリティチップを使用する [ユーザ] を登録します。
セキュリティチップは、各ユーザに固有の鍵を生成し、証明書を管理します。この鍵と証明書を用いることにより、セキュリティチップは暗号化や認証を行います。セキュリティチップ内に保有する鍵は、取り出すことが不可能なため、鍵の解読ができず、そのため暗号化されたデータや認証は安全に行われます。ユーザはこの鍵と証明書を利用するためのパスワードを設定します。
所有者およびユーザは以下の鍵および証明書やファイルを作成・利用します。

□［所有者］が管理するもの

所有者キーと所有者パスワード

所有者は、所有者であることを証明するキーを作成します。この鍵はセキュリティチップにより保護され、所有者パスワードを入力することによって利用することができます。所有者パスワードは忘れないよう十分注意してください。

緊急時復元用アーカイブファイル

所有者は、ユーザに対しセキュリティチップを利用する権限を与えます。所有者は利用権をもつユーザのリストを作成し、仮にセキュリティチップに不具合が発生しても、このリストをもとにユーザの利用権を復元することができます。所有者はこのリストを緊急時復元用アーカイブとしてファイル保存し、セキュリティチップの不具合発生時に備えます。緊急時復元用アーカイブは、他人に読めないよう暗号化されて保存されます。

緊急時復元用アーカイブファイルを復元するトークン

緊急時復元用アーカイブは暗号化されて保存されます。これを利用するには復号化が必要ですが、その際トークン鍵を利用します。トークン鍵は、暗号化されたアーカイブを復元するための鍵で、パスワードによって保護されます。トークン鍵およびパスワードを紛失した場合は、ユーザの再登録ができなくなります。また、他人に渡らないよう十分注意して管理してください。

□［ユーザ］が管理するもの

ユーザーキーとユーザーキーパスワード

ユーザはセキュリティチップを利用する際、ユーザーキーを作成します。この鍵はセキュリティチップにより保護され、ユーザーキーパスワードを入力することによって利用することができます。鍵を紛失した場合は、それ以前に暗号化していたデータやファイル等を再び利用することができなくなります。管理には十分注意してください。また、パスワードを忘れた場合も、鍵が利用できなくなるため、それまでに暗号化していたデータやファイルを再び利用することができなくなります。パスワードは忘れないよう十分注意してください。

重要

- ユーザが暗号化したデータは、所有者からも見ることができないよう保護するため、ユーザーキーパスワードは所有者でも利用できないようになっています。このため、パスワード忘却時は所有者でも復元（復号）化できないようになっています。十分注意して管理してください。

キーのバックアップ

キーを紛失した場合に備え、バックアップファイルを作成することが可能です。バックアップファイルはユーザーキーパスワードによって保護されます。

■セキュリティチップの利用

セキュリティチップを利用するために、次のアプリケーションおよび証明書を使用します。

・Infineon TPM Professional Package（Infineon Security Platform）
・SMARTACCESS/Trust
・VeriSign 証明書

これらのアプリケーションおよび証明書により、以下のことが行えるようになります。

□ファイルとフォルダの暗号化 -EFS（Encrypting File System）

Infineon Security Platform でファイルとフォルダの暗号化を設定することにより、EFS による暗号化に利用される鍵をセキュリティチップにて安全に保管します。

重要

- EFS を利用するには、ハードディスクが NTFS でフォーマットされている必要があります。フォーマットの変更方法はパソコン本体の『FMV マニュアル』の「機能」を参照ください。
- Windows XP Home Edition では、EFS は利用できません。

□セキュア E-Mail

Infineon Security Platform で電子メールの保護を設定することにより、E-Mail の暗号用の証明書をセキュリティチップにて安全に管理します。

□Word マクロへの署名

Infineon Security Platform でセキュリティ機能を設定することにより、Word マクロへの署名をセキュリティチップで安全に保護します。

□Windows ログオンにセキュリティチップを利用する

SMARTACCESS/Trust で Trusted ログオンを設定することにより、Windows ログオン時のパスワードをセキュリティチップにて安全に保存することができます。

□ パソコンの不正なハードウェアの変更の検出

SMARTACCESS/Trust の「機器監査」機能を利用すれば、Windows ログオン時パソコンの機器構成のチェックを行います。ハードウェア構成または設定が不正に変更されていることを検出した場合は、Windows ログオンを許可しないようにすることができます。

□ ID・パスワード入力をセキュリティチップで管理する

ID・パスワードの入力が必要な以下の場合に、ID・パスワードを SMARTACCESS/Trust に登録しておくと、セキュリティチップによって保護されるため、安全に管理することができます。

・アプリケーションによりポップアップ画面に表示される ID・パスワード入力要求

・Internet Explorer によりホームページに表示される ID・パスワード入力要求

また、一度登録すると、ID やパスワードのフォームは自動で認識され、再び手入力することなく利用できます。

□ シングルサインオンを利用する

SMARTACCESS/Trust にはシングルサインオンの機能があります。一度セキュリティチップのパスワードを入力するか、Trusted ログオンを行えば、SMARTACCESS/Trust が管理する ID やパスワードは自動で入力されます。

□ VeriSign 証明書の利用

セキュリティチップと連携した VeriSign 発行の証明書を、登録した日から 1 年間無料で利用できます。これを利用することにより、例えばセキュア E-mail を利用する際などは、VeriSign 認証局に証明された証明書を利用できるため、より安全なデータを送受信することができます。

POINT

- VeriSign 証明書は、セキュリティチップのユーティリティをインストールし、設定を完了して利用可能にしてからインストールを行ってください。インストールについて詳しくは、ドライバーズディスク内の「¥other¥tpm¥ifxsw17¥verisign.txt」をご覧ください。
- VeriSign 証明書は、登録した日から 1 年間利用できます。それ以降は、E-mail 等で証明書を利用することはできません。ただし、古いメール等で利用していた場合には、読むことのみ可能です。
- 1 年間の利用期間終了後もご利用を希望の場合は、弊社担当営業員までご連絡ください。その場合有料による継続となります。

□ セキュリティチップとスマートカードを連携して利用

カスタムメイドや別売のスマートカードをご購入された場合、連携した利用が可能です。

重要

- スマートカードと連携して利用するには、スマートカード用アプリケーション SMARTACCESS/BASE または SMARTACCESS/PRO が必要です。
- スマートカードと連携して利用するには、SMARTACCESS/Trust より先に、SMARTACCESS/BASE または SMARTACCESS/PRO をインストールする必要があります。詳しくは SMARTACCESS/Trust のマニュアルを参照してください。

2 作業の流れ

本製品を使用するまでの手順は以下のとおりです。

1 必要なものを用意します。

・パソコン本体
・ドライバーズディスク

2 BIOS の設定を変更します。

「BIOS の設定を変更する」（→ P.11）

1. BIOS の「管理者用パスワード」を設定します。
2. セキュリティチップを「使用する」に設定します。

3 ユーティリティをインストールします。

「ユーティリティをインストールする」（→ P.14）

4 ユーティリティの設定を行います。

「ユーティリティの設定を行う」（→ P.16）
「ユーティリティの確認を行う」（→ P.18）

1. 所有者のパスワードを設定します。
2. 緊急時復元用アーカイブを保存します。
3. 緊急時復元用トークンのパスワードを設定します。
4. 緊急時復元用トークンを保存します。
5. 基本ユーザーキーパスワードを設定します。
6. 電子メールの保護と、ファイルとフォルダの暗号化を設定します。
7. 設定の確認を行います。

5 アプリケーションをインストールします。

「アプリケーションをインストールする」（→ P.18）

6 アプリケーションの設定を行います。

「アプリケーションの設定を行う」（→ P.19）

1. Trusted ログオンを設定します。
2. 機器構成を登録し、機器監査を設定します。
3. 一時中止パスワードを設定します。
4. Windows ログオンを Trusted ログオンに変更します。

3 動作条件

本製品をご使用になる前に、次の条件を確認してください。

■ 対応機種／ OS

本製品が搭載されている FMV パソコン／ Windows XP/2000

POINT

- WEB ページをご覧になるためのアプリケーションとして、Internet Explorer 6.0 以降または Netscape 4.78/7.0 以降が必要です。
- セキュア E-mail を利用するには、Outlook 2000/2002 以降、Outlook Express 6.0 以降、または Netscape 4.78/7.0 以降が必要です。
- Word マクロへの署名を利用するには、Word 2000/2002 以降が必要です。
- VeriSign 証明書を利用するには、Internet Explorer 6.0 または Netscape 4.78/7.0 が必要です。
- SMARTACCESS/Trust での、アプリケーションによりポップアップ画面に表示される ID・パスワード入力要求機能は、Netscape ではお使いになれません。

4 インストールを行う

BIOS の設定を変更する

本製品を使用する前に、必ず BIOS の設定を変更してください。

・「E635 の場合」（→ P.11）
・「E630、K630 の場合」（→ P.12）
・「NA/H、NA/L、MG/H、MT の場合」（→ P.13）

POINT

- BIOS セットアップについて詳しくは、パソコン本体の『FMV マニュアル』の「BIOS」を参照してください。

■ E635 の場合

1 パソコン本体の電源を入れ、BIOS セットアップを起動します。

BIOS セットアップ画面が表示されます。
BIOS セットアップで管理者用パスワードを設定済の場合は、手順 7 へ進んでください。設定していない場合には、手順 2 へ進んでください。

重要

- 本製品を使用するには､BIOSセットアップで管理者用パスワードを設定する必要があります。

2 Security メニューで「Set Supervisor Password」を選択して、【Enter】キーを押します。

パスワード入力用のウィンドウが表示されます。

3 8 桁までのパスワードを入力します。

入力できる文字種はアルファベットと数字です。
入力された文字は表示されず、代わりに「＊」が表示されます。

4 パスワードを入力したら、【Enter】キーを押します。

「Confirm New Password」が表示され、パスワードの再入力を求められます。

5 手順 3 で入力したパスワードを再度入力して【Enter】キーを押します。

「Password Installed」と書かれたウィンドウが表示されます。

6 【Enter】キーを押します。

再入力したパスワードが間違っていた場合は、「Passwords do not match!」と書かれたウィンドウが表示されます。【Enter】キーを押して、手順 3 からやり直してください。

7 【↑】キーまたは【↓】キーでカーソルを移動し、「Security Chip」を選択して【Enter】キーを押します。

設定変更画面が表示されます。

8 【↑】キーまたは【↓】キーを押して、「Enabled」に設定します。

9 Exit メニューが表示されるまで、何度か【Esc】キーを押します。

10 【↑】キーまたは【↓】キーを押して「Exit Saving Changes」を選択し、【Enter】キーを押します。

「Save Configuration Changes and exit now?」と書かれたウィンドウが表示されます。

11 【←】キーまたは【→】キーを押して「Ok」を選択し、【Enter】キーを押します。

BIOS セットアップが終了し、パソコン本体が再起動します。

重要

セキュリティチップの設定を有効にするには、BIOS セットアップ終了後にパソコン本体の再起動が必要です。

■E630、K630 の場合

1 パソコン本体の電源を入れ、BIOS セットアップを起動します。

BIOS セットアップ画面が表示されます。

BIOS セットアップで管理者用パスワードを設定済の場合は、手順 7 へ進んでください。設定していない場合には、手順 2 へ進んでください。

重要

- 本製品を使用するには、BIOSセットアップで管理者用パスワードを設定する必要があります。

2 Security メニューで「Set Supervisor Password」を選択して、【Enter】キーを押します。

パスワード入力用のウィンドウが表示されます。

3 8 桁までのパスワードを入力します。

入力できる文字種はアルファベットと数字です。

入力された文字は表示されず、代わりに「■」が表示されます。

4 パスワードを入力したら、【Enter】キーを押します。

「Confirm New Password」にカーソルが移り、パスワードの再入力を求められます。

5 手順 3 で入力したパスワードを再度入力して【Enter】キーを押します。

「Setup Notice」と書かれたウィンドウが表示されます。

6 【Enter】キーを押します。

再入力したパスワードが間違っていた場合は、「Setup Warning」と書かれたウィンドウが表示されます。【Enter】キーを押して、手順 3 からやり直してください。

7 【↑】キーまたは【↓】キーでカーソルを移動し、「Security Chip Setting」を選択して【Enter】キーを押します。

設定変更画面が表示されます。

8 【Space】キーまたは【−】キーを押して、「Security Chip」の項目を「Enabled」に設定します。

9 Exit メニューが表示されるまで、何度か【Esc】キーを押します。

10 【↑】キーまたは【↓】キーを押して「Exit Saving Changes」を選択し、【Enter】キーを押します。

「Save Configuration Changes and exit now?」と書かれたウィンドウが表示されます。

11 【←】キーまたは【→】キーを押して「Yes」を選択し、【Enter】キーを押します。

BIOS セットアップが終了し、パソコン本体が再起動します。

重要

セキュリティチップの設定を有効にするには、BIOS セットアップ終了後にパソコン本体の再起動が必要です。終了メニューで「Exit Saving Changes」を行っただけで電源を切ってしまうと、設定が正しく行われませんのでご注意ください（次回起動時にエラーメッセージが表示されます）。

■ NA/H、NA/L、MG/H、MT の場合

1 パソコン本体の電源を入れ、BIOS セットアップを起動します。

「BIOS セットアップ画面」が表示されます。

BIOS セットアップで管理者用パスワードを設定済の場合は、手順 7 へ進んでください。設定していない場合には、手順 2 へ進んでください。

重要

- 本製品を使用するには、BIOS セットアップで管理者用パスワードを設定する必要があります。

2 セキュリティメニューで「管理者用パスワード設定」を選択して、【Enter】キーを押します。

パスワード入力用のウィンドウが表示されます。

3 8 桁までのパスワードを入力します。

入力できる文字種はアルファベットと数字です。

入力された文字は表示されず、代わりに「■」が表示されます。

4 パスワードを入力したら、【Enter】キーを押します。

「新しいパスワードを確認してください。」にカーソルが移り、パスワードの再入力を求められます。

5 手順 3 で入力したパスワードを再度入力して【Enter】キーを押します。

「セットアップ通知」と書かれたウィンドウが表示されます。

6 **【Enter】キーを押します。**

再入力したパスワードが間違っていた場合は、「セットアップ警告」と書かれたウィンドウが表示されます。【Enter】キーを押して、手順 3 からやり直してください。

7 **【↑】キーまたは【↓】キーでカーソルを移動し、「セキュリティチップ設定」を選択して【Enter】キーを押します。**

「セキュリティチップ設定」が表示されます。

8 **【Space】キーまたは【−】キーを押して、「セキュリティチップ」の項目を「使用する」に設定します。**

9 **終了メニューが表示されるまで、何度か【Esc】キーを押します。**

10 **【↑】キーまたは【↓】キーを押して「変更を保存して終了する」を選択し、【Enter】キーを押します。**

「セットアップ確認」と書かれたウィンドウが表示されます。

11 **【←】キーまたは【→】キーを押して「はい」を選択し、【Enter】キーを押します。**

BIOS セットアップが終了し、パソコン本体が再起動します。

重要

- 「セキュリティチップ」の設定を有効にするには、BIOS セットアップ終了後にパソコン本体の再起動が必要です。終了メニューで「変更を保存する」を行っただけで電源を切ってしまうと、設定が正しく行われませんのでご注意ください（次回起動時にエラーメッセージが表示されます）。

ユーティリティをインストールする

BIOS の設定変更後、パソコン本体が再起動したら、Infineon TPM Professional Package (Infineon Security Platform) ユーティリティをインストールします。

重要

- ユーティリティをインストールするには、管理者権限で Windows にログオンする必要があります。
- Windows 2000 の再インストールを行った場合、BIOS セットアップでセキュリティチップを「Enabled」（E635、E630、K630 の場合）または「使用する」（NA/H、NA/L、MG/H、MT の場合）に設定した後、最初に Windows を起動すると「新しいハードウェアの検出ウィザード」が表示されます。このウィザードが表示された場合はキャンセルしてください。

POINT

- ユーティリティをインストールする前に、他の使用中のアプリケーションはすべて終了させてください。

1 「ドライバーズディスク」をセットします。

POINT

- Windows XP では Windows 起動中に「ドライバーズディスク」をセットすると、「Windows が実行する動作を選んでください」と表示されます。「キャンセル」をクリックしてください。

2 「スタート」ボタン→「ファイル名を指定して実行」の順にクリックします。

3 「名前」の欄に次のように入力し、「OK」をクリックします。

[CD-ROM ドライブ]:¥other¥tpm¥ifxsw17¥install.bat

「Infineon TPM Professional Package 用の InstallShield ウィザードへようこそ」が表示されます。

4 「次へ」をクリックします。

「ライセンス契約」が表示されます。

5 「はい」をクリックします。

「ユーザ情報」が表示されます。

6 ユーザ名と所属を入力し、「次へ」をクリックします。

「セットアップタイプ」が表示されます。

POINT

- 所属は省略することもできます。

7 「カスタム」を選択し、「次へ」をクリックします。

「カスタムセットアップ」が表示されます。

8 「次へ」をクリックします。

「プログラムをインストールする準備ができました」と表示されます。

POINT

- 「カスタムセットアップ」では何も変更する必要はありません。

9 「インストール」をクリックします。

インストールが開始します。しばらくして、インストールが終了すると、「InstallShield ウィザードを完了しました」が表示されます。

10 「完了」をクリックします。

メモ帳が表示されます。読み終わったらメモ帳を終了してください。再起動を要求するメッセージが表示されます。

11 「はい」をクリックします。

パソコン本体が再起動します。

ユーティリティの設定を行う

ユーティリティのインストール終了後、パソコン本体が再起動したら、ユーティリティで「プラットフォーム初期化ウィザード」を行い、セキュリティチップの所有者を設定します。その後「ユーザー初期化ウィザード」にてユーザの設定を行います。

重要

- ユーティリティの設定を行うには、管理者権限を持ったユーザーとして Windows にログオンする必要があります。

1 管理者権限を持ったユーザーとして、Windows にログオンします。

通知領域（Windows XP の場合）またはタスクトレイ（Windows 2000 の場合）の「Infineon Security Platform」アイコンから、「Security Platform が初期化されていません」というメッセージが表示されます。

2 通知領域（Windows XP の場合）またはタスクトレイ（Windows 2000 の場合）の「Infineon Security Platform」アイコンをクリックします。

メニューが表示されます。

3 「Security Platform の初期化」を選択します。

「Infineon Security Platform 初期化ウィザードにようこそ」が表示されます。
表示されない場合は、「スタート」ボタン→「(すべての）プログラム」→「Infineon Security Platform ツール」→「Security Platform 初期化ウィザード」をクリックします。

4 「既存の Security Platform を復元する」がチェックされていないことを確認し、「次へ」をクリックします。

「所有者権限の設定」が表示されます。

5 所有者の「パスワード」と「パスワードの確認入力」に入力し、「次へ」をクリックします。

「緊急時復元プロセスの設定」が表示されます。

6 「新しい復元用アーカイブを作成する」をチェックして、保存場所を確認し、「次へ」をクリックします。

「Security Platform の緊急時復元用トークンのパスワードを入力」が表示されます。

重要

- 緊急時復元用アーカイブの保存場所は通常、表示されている場所から変更する必要はありません。

7 緊急時復元用トークンの「パスワード」と「パスワードの確認入力」に入力し、「次へ」をクリックします。

「復元用トークンの保存」が表示されます。

8 緊急時復元用トークンの保存場所を設定し、「次へ」をクリックします。

「サマリー」が表示されます。

重要

- 保存先は仮の場所が表示されています。緊急時復元用トークンは、リムーバブルドライブ等、パソコン本体とは別の場所に保管できる媒体に保存することをお勧めします。

9 **「次へ」をクリックします。**

しばらくすると、「ウィザードが正常に終了しました。」が表示されます。

10 **「Security Platform ユーザー初期化ウィザードを起動する」をチェックして「完了」をクリックします。**

「Infineon Security Platform ユーザー初期化ウィザードにようこそ」が表示されます。

11 **「次へ」をクリックします。**

「基本ユーザーキーパスワード」が表示されます。

12 **基本ユーザーキーの「パスワード」と「パスワードの確認入力」に入力し、「次へ」をクリックします。**

「設定の確認」が表示されます。

13 **「次へ」をクリックします。**

しばらくすると、「Security Platform の機能」が表示されます。

14 **「電子メールの保護」、「ファイルとフォルダの暗号化 (EFS)」にチェックが入っていることを確認し、「次へ」をクリックします。**

「電子メールの保護に関する設定」が表示されます。

重要

- 「電子メールの保護」と「ファイルとフォルダの暗号化 (EFS)」の他に「Personal Secure Drive」が表示されていることがありますが、チェックしないでください。本機能はサポートしていません。
- Windows XP Home Edition をお使いの場合は、「ファイルとフォルダの暗号化 (EFS)」は選択できません。

15 **「次へ」をクリックします。**

「暗号化証明書」が表示されます。

16 **「発行先」が自分になっていることを確認し、「次へ」をクリックします。**

「設定の確認」が表示されます。

17 **「次へ」をクリックします。**

しばらくすると、「ウィザードが正常に終了しました。」が表示されます。

18 **「完了」をクリックします。**

「今すぐ再起動しますか？」が表示されます。

19 **「はい」をクリックします。**

パソコン本体が再起動します。

以上で、Infineon Security Platform ツールによる TCG セキュリティ機能が利用できる環境が整いました。

ユーティリティの確認を行う

ユーティリティのインストールと設定が完了したら、次の手順で正しく設定されたか確認してください。

1 **「スタート」ボタン→「（すべての）プログラム」→「Infineon Secure Platform ツール」の「Security Platform 設定ツール」の順にクリックします。**

「Infineon Security Platform 設定ツール」が表示されます。

2 **「全般」タブをクリックします。**

3 **「Security Platform の状態」が次の状態になっていることを確認します。**

「チップ」：有効
「所有者」：初期化完了
「ユーザー」：初期化完了

4 **「OK」をクリックし、「Infineon Security Platform 設定ツール」を終了します。**

アプリケーションをインストールする

ユーティリティの設定が完了したら、SMARTACCESS/Trust アプリケーションをインストールします。

重要

- アプリケーションをインストールするには、管理者権限で Windows にログオンする必要があります。

POINT

- アプリケーションをインストールする前に、他の使用中のアプリケーションはすべて終了させてください。

1 **「ドライバーズディスク」をセットします。**

POINT

- Windows XP では Windows 起動中に「ドライバーズディスク」をセットすると、「Windows が実行する動作を選んでください」と表示されます。「キャンセル」をクリックしてください。

2 **「スタート」ボタン→「ファイル名を指定して実行」の順にクリックします。**

3 「名前」の欄に次のように入力し、「OK」をクリックします。

[CD-ROMドライブ]：¥other¥tpm¥satrust¥setup.exe

「SMARTACCESS/Trust V1.0L20 をコンピュータにインストールします。」が表示されます。

4 「次へ」をクリックします。

「セットアップは次のフォルダに SMARTACCESS/Trust V1.0L20 をインストールします。」が表示されます。

5 インストール先のフォルダを選択して、「次へ」をクリックします。

インストールが開始されます。
しばらくすると、「SMARTACCESS/Trust V1.0L20 のインストールを完了しました。」が表示されます。

POINT

- インストール先のフォルダは通常、変更する必要はありません。変更すると不都合が発生することもあるため、パソコンに詳しい方以外は変更しないでください。

6 「完了」をクリックします。

再起動を要求するメッセージが表示されます。

7 「はい」をクリックします。

パソコンが再起動します。

アプリケーションの設定を行う

アプリケーションのインストールが終わったら、アプリケーションの設定を行います。
アプリケーションにより Windows のログオンパスワード等をセキュリティチップに保存するので、パスワードを安全に管理できます。

POINT

- 必ず管理者でログオンしてください。
- 他のアプリケーションはすべて終了させてください。
- 他のセキュリティ機能により Windows ログオンを行っている場合は、その利用を止めてから設定するか、セキュリティチップにて行うのを止めてください。
- アプリケーションの設定について詳しくは、SMARTACCESS/Trust アプリケーションのマニュアルを参照してください。

重要

- 設定の途中で、現在のパソコンの機器構成を登録する作業を行います。
  機器構成を登録すると、現在の BIOS ハードウェア設定等を保存します。登録を行う前に BIOS 設定を含めたハードウェア設定（機器構成）を完了してから行ってください。

1 「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS Trust」→「ログオン設定ツール」の順にクリックします。

「ログオン設定ツール」が表示されます。

2 **ユーザーキーパスワードを入力し「OK」をクリックします。**

3 **「Trusted ログオン」の「登録」をクリックします。**

「Trusted ログオン情報登録」が表示されます。

4 **「Windows ログオン」に、Windows ログオン時の「ユーザー名」、「ドメイン名」、「パスワード」、および「パスワード確認入力」を入力します。**

POINT

- ドメインを利用していない場合は「ドメイン名」の入力は不要です。

5 **「ユーザーキーパスワード」に、登録するユーザーキーパスワードを入力し、「OK」をクリックします。**

「Trusted ログオン情報を設定しました。」が表示されます。

6 **「OK」をクリックします。**

「ログオン設定ツール」に戻ります。

□ 機器監査の設定を行う

つづいて、機器監査の設定を行います。機器監査の設定を行わない場合は、「シングルサインオンの設定を行う」（→ P.21）に進んでください。

7 **「Trusted ログオン」の「機器構成設定」をクリックします。**

「Trusted ログオン機器構成情報登録」が表示されます。

8 **「現状登録」をクリックします。**

「現在の機器構成を登録しますか？」が表示されます。

9 **「はい」をクリックします。**

「Trusted ログオン機器構成情報登録」に戻ります。

重 要

- Windows が起動される直前の機器構成が登録されます。モバイルマルチベイ／マルチベイの変更（NA/H、NA/L、MG/H、MT の場合）など、Windows の起動後に行った機器の変更は登録されませんのでご注意ください。

10 **「起動時に機器監査実行」をチェックします。**

11 **「起動時に機器構成が異なる場合のログオン」を「ログオンしない」にチェックして、「OK」をクリックします。**

「ログオン設定ツール」に戻ります。

重 要

- 機器監査で検出されるハードウェアの変更については、「機器監査について」（→ P.26）を参照してください。機器構成を不用意に変更すると、ログオンが行えなくなる可能性がありますので十分にご注意ください。再度、機器構成の変更が必要となった場合は、必ず「起動時に機器監査実行」を一度オフにしてから行ってください。

12 「一時中止パスワード」をクリックし、パスワードを入力し、「OK」をクリックします。

「一時中止パスワードを登録しました。」が表示されます。

重要

- 一時中止パスワードは、セキュリティチップに不具合が発生したときなどTrustedログオンができなくなった場合に、一時的に Windows ログオンに切り替えるための手段です。
- 一時中止パスワードで Windows にログオンしても、セキュリティチップによって暗号化されたファイル等は、安全に保護されています。これらファイルは、ユーザーキーパスワードを入力するまで見ることができません。

13 「OK」をクリックします。

「ログオン設定ツール」に戻ります。

□ シングルサインオンの設定を行う

つづいて、シングルサインオンの設定を行います。シングルサインオンの設定を行わない場合は、手順 16 に進んでください。

14 「その他」の「動作環境設定」をクリックします。

「動作環境設定」が表示されます。

15 「シングルサインオン」の「有効にする」にチェックし、「OK」をクリックします。

「ログオン設定ツール」に戻ります。

16 「ログオン方法変更」をクリックし、「Trusted　ログオン」を「使用する」にチェックし、「OK」をクリックします。

「本製品以外のログオン認証が有効になっている場合・・・」の確認画面が表示されます。

17 「OK」をクリックします。

「ログオン方法を変更しました。」が表示されます。

18 「OK」をクリックします。

「ログオン設定ツール」に戻ります。

19 「閉じる」をクリックします。

「今すぐ再起動しますか」が表示されます。

20 「はい」をクリックします。

パソコンが再起動します。

POINT

- 設定後は、Windows ログオン画面は「ようこそ」表示から「クラシック」表示に切り替わります。
- Windows ログオンの方法は以下の手順になります。
  1. Windows を起動後、画面の指示に従い、【Ctrl】+【Alt】+【Del】キーを押します。
     「Trusted ログオン」画面が表示されます。
  2. ユーザー名とユーザーキーパスワードを入力します。
     Windows にログオンします。

5 運用上の注意

TCG によるセキュアな環境を運用するときは、次の点に注意して管理・運用してください。

パスワードの変更

所有者パスワードまたはユーザーキーパスワードの変更は、以下の方法で行います。

POINT

- セキュリティチップのパスワードは、セキュリティ面を考慮し、定期的に変更することをお勧めします。

■所有者パスワードの変更方法

1 **通知領域（Windows XP の場合）またはタスクトレイ（Windows 2000 の場合）の「Infineon Security Platform」アイコンをクリックし、表示されるメニューから「Security Platform の管理」を選択します。**
「Infineon Security Platform 設定ツール」が表示されます。

2 **「アドバンス」タブを選択し、「所有者のパスワード」の「変更」をクリックします。**
以降の操作は画面の指示に従ってください。

■ユーザーキーパスワードの変更方法

1 **通知領域（Windows XP の場合）またはタスクトレイ（Windows 2000 の場合）の「Infineon Security Platform」アイコンをクリックし、表示されるメニューから「Security Platform の管理」を選択します。**
「Infineon Security Platform 設定ツール」が表示されます。

2 **「ユーザー設定」タブを選択し、「基本ユーザーキーのパスワード」の「変更」をクリックします。**
以降の操作は画面の指示に従ってください。

緊急時復元用アーカイブおよびトークンの管理

■緊急時復元用アーカイブ

緊急時復元用アーカイブは所有者が管理するユーザのリストです。コピーをリムーバブルディスクやサーバ等に置き、なくさないよう管理してください。また、アーカイブはユーザを追加したりパスワードを変更するなど、ユーザ情報を変更するたびに更新されます。アーカイブは定期的にコピーをとってください。なお、アーカイブはトークンにより暗号化されているので、他の人に見られてもセキュリティ上問題ありません。

■緊急時復元用トークン

緊急時復元用トークンは暗号化されたアーカイブを復元化するための鍵です。トークンはパスワードにより保護されています。アーカイブを復元する際に必要ですので、リムーバブルディスク等に保存し、なくさないよう注意してください。また、パスワードを他の人にわからないよう注意して保管してください。

ユーザーキーをバックアップ／復元する

ユーザの鍵は、新規に証明書を取得するたびに新しい鍵が作成され、構成が変わります。このため、鍵の破損時の復旧に備え、定期的に鍵のバックアップを取ることをお勧めします。

POINT

- 操作について詳しくは、Infineon Security Platform ツールのバックアップのマニュアルを参照してください。

重要

- 鍵を破損、紛失すると、以前に暗号化したファイルを再び参照することができなくなります。

■鍵をバックアップする

1 通知領域（Windows XP の場合）またはタスクトレイ（Windows 2000 の場合）の「Infineon Security Platform」アイコンをクリックし、表示されるメニューから「Security Platform の管理」を選択します。

「Infineon Security Platform 設定ツール」が表示されます。

2 「バックアップ」タブを選択し、「バックアップ」をクリックします。

「キーと証明書をバックアップする」が表示されます。

3 「参照」をクリックし、鍵（ファイル）をバックアップする場所を選択します。

重要

- 所有者は、「緊急時復元用アーカイブをバックアップデータに追加」にチェックをしてください。

4 「次へ」をクリックします。

「サマリー」が表示されます。

5 「次へ」をクリックします。

鍵(ファイル)が保存されると、「ウィザードが正常に終了しました」が表示されます。

6 「完了」をクリックします。

■鍵を復元する

1 通知領域(Windows XP の場合)またはタスクトレイ(Windows 2000 の場合)の「Infineon Security Platform」アイコンをクリックし、表示されるメニューから「Security Platform の管理」を選択します。

「Infineon Security Platform 設定ツール」が表示されます。

2 「バックアップ」タブを選択し、「復元」をクリックします。

「設定を復元する」が表示されます。

3 「参照」をクリックし、復元する鍵(ファイル)の場所を選択します。

4 「次へ」をクリックします。

「サマリー」が表示されます。

5 「次へ」をクリックします。

鍵(ファイル)が復元されると、「ウィザードが正常に終了しました。」が表示されます。

6 「Security Platform ユーザー初期化ウィザードを起動する」にチェックが入っていることを確認し、「完了」をクリックします。

「Security Platform の機能」が表示されます。

7 「ユーティリティの設定を行う」手順 14(→ P.17)以降の手順に従い、再設定します。

コンピュータから離れるとき(離席時)

コンピュータから離れる場合は、他人にコンピュータを操作されないよう注意が必要です。以下の設定を施すことで、離席時でもコンピュータはセキュリティチップにより安全に保護されます。

■スクリーンセーバーのパスワード

スクリーンセーバーを設定する際、「パスワードによる保護」を行えば、パスワードはセキュリティチップにより安全に保護されます。設定方法は、Windows のマニュアルを参照ください。

■ コンピュータのロック

コンピュータのロック（Windows XP の場合）またはワークステーションのロック（Windows 2000 の場合）を行えば、復帰時のパスワードはセキュリティチップにより安全に保護されます。

■ スタンバイや休止状態から回復するときのパスワード

スタンバイや休止状態の設定をしている場合、「スタンバイから回復するときにパスワードの入力を求める」を設定しておくと、パスワードはセキュリティチップにより安全に保護されます。設定方法は、Windows のマニュアルを参照してください。

機器監査について

SMARTACCESS/Trust にて「起動時に機器監査実行」を設定しておくと、パソコンの電源を入れたときやパソコンを再起動したときにハードウェアが変更されていることを検出すると、Windows のログオンを禁止することができます。これにより、ユーザが気づかないうちに（帰宅時等）ハードウェアに何らかの変更がされても、変更されたことを検出することができます。

重要

- 以下に示す変更を行う場合は、前もって SMARTACCESS/Trust の「起動時に機器監査実行」をオフにし、変更した後に再度「現状登録」を行う必要があります。設定方法については、「アプリケーションの設定を行う」（→ P.19）および SMARTACCESS/Trust のマニュアルを参照してください。

POINT

- ハードウェアが変更されているかどうかは、休止状態からの復帰時にも確認されます。

ハードウェアの変更については以下の項目が検出されます。

□ BIOS 設定変更

BIOS にてハードウェア構成が変更された場合には、機器監査にて通知されます。

□ メモリ構成の変更

メモリスロットの構成に変更があった場合には、機器監査にて通知されます。

□ PCI スロット、グラフィックボードの変更（E635、E630、K630 の場合）

PCI スロットの構成およびグラフィックボードを変更した場合には、機器監査にて通知されます。

□ モバイルマルチベイ／マルチベイの変更（NA/H、NA/L、MG/H、MT の場合）

モバイルマルチベイまたはマルチベイを変更した場合には、機器監査にて通知されます。

□ USB デバイスの変更（E635 以外の場合）

USB ポートに USB メモリなどのストレージデバイスを接続した場合には、機器監査にて通知されます。

POINT

- USB デバイスの変更を検出するには、BIOS セットアップで次のように設定する必要があります。
  - ・E630、K630 の場合
    「USB Legacy Emulation」: Enabled
  - ・NA/H、NA/L、MG/H、MT の場合
    「レガシー USB サポート」: 使用する

  BIOS セットアップについて詳しくは、パソコン本体の『FMV マニュアル』の「BIOS」を参照してください。

6 こんなときには

新規ユーザの登録

Windows に新規ユーザを追加した場合、そのユーザがセキュリティ環境を利用できるよう登録する必要があります。
以下の方法で、Infineon Security Platform ユーティリティより、セキュリティチップにユーザを登録し、その後、SMARTACCESS/Trust へユーザ登録します。

POINT

- Trusted ログオンを設定している場合は、一度「一時中止パスワード」にて Windows にログオンする必要があります。所有者にご相談ください。
- 事前に Windows にユーザを追加しておく必要があります。管理者にご相談ください。
- Windows で新規ユーザを「ユーザーは次回ログオン時にパスワードの変更が必要」で作成した場合は、新規ユーザのログオン前に一度 Trust ログオンを解除してください。Windows のパスワードを変更した後で、再度 Trust ログオンを設定してください。

■ユーティリティへの登録

1. **登録するユーザーで、Windows にログオンします。**
   通知領域（Windows XP の場合）またはタスクトレイ（Windows 2000 の場合）の「Infineon Security Platform」アイコンから「現在のユーザ用に Security Platform が初期化されていません」というメッセージが表示されます。

2. **通知領域（Windows XP の場合）またはタスクトレイ（Windows 2000 の場合）の「Infineon Security Platform」アイコンをクリックします。**
   メニューが表示されます。

3. **「Security Platform のユーザの初期化」を選択します。**
   「Infineon Security Platform ユーザー初期化ウィザードにようこそ」が表示されます。
   表示されない場合は「スタート」ボタン→「（すべての）プログラム」→「Infineon Security Platform ツール」→「Security Platform ユーザー初期化ウィザード」をクリックします。

4. **「ユーティリティの設定を行う」の手順 11（→ P.17）以降を行い、登録します。**
   「基本ユーザーキーのパスワード」が表示されます。

5. **「ユーティリティの確認を行う」（→ P.18）の手順で、ユーティリティが正しく設定されたか確認してください。**

POINT

- Trusted ログオンを設定している場合は、「一時中止パスワード」にて Windows にログオンする必要があります。管理者にご相談ください。

■アプリケーションの設定

引き続き、SMARTACCESS/Trust に登録します。

POINT

- Trusted ログオンを設定している場合は、「一時中止パスワード」にて Windows にログオンする必要があります。管理者にご相談ください。

1 **「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS Trust」→「ログオン設定ツール」の順にクリックします。**

2 **ユーザーキーパスワードを入力し「次へ」をクリックします。**

「ログオン設定ツール」が表示されます。

3 **「Trusted ログオン」の「登録」をクリックします。**

「Trusted ログオン情報登録」が表示されます。

4 **Windows ログオン時の「ドメイン名」、「パスワード」、および「パスワード確認入力」を入力します。**

POINT

- ドメインを利用していない場合は、「ドメイン名」の入力は不要です。

5 **「OK」をクリックします。**

「Trusted ログオン情報を設定しました。」が表示されます。

6 **「OK」をクリックします。**

「ログオン設定ツール」に戻ります。

7 **「閉じる」をクリックします。**

セキュリティチップ破損等によるパソコン修理後の作業について

セキュリティチップの不具合などによりパソコンの修理を依頼した場合など、返却時セキュリティチップに以前の情報を復元する必要がある場合があります。その際には以下の手順で行います。

・所有者は所有者キーを生成し、緊急時復元用ファイルを作成します。

・ユーザは鍵を再登録し、環境を再構築します。

重要

- この操作はハードディスクが交換されていないことが前提です。
- セキュリティチップの情報を復元するには、緊急時復元用のアーカイブとトークンがバックアップ（保存）されている必要があります。
- 操作を行う前に、BIOS の設定でセキュリティチップが「Enabled」（E635、E630、K630 の場合）または「使用する」（NA/H、NA/L、MG/H、MT の場合）になっていることを確認してください。（「BIOS の設定を変更する」（→ P.11））

POINT

- 操作について詳しくは、Infineon Security Platform ツールの緊急時復元用機能のマニュアルを参照してください。

■所有者環境の再構築

POINT

- 事前に以下を確認してください。
  - ・所有者パスワード
  - ・緊急時復元用アーカイブ
  - ・緊急時復元用トークンとそのパスワード
- Trusted ログオンを設定している場合は、「一時中止パスワード」にて Windows にログオンする必要があります。

1 **パソコンの電源を入れます。**

通知領域（Windows XP の場合）またはタスクトレイ（Windows 2000 の場合）の「Infineon Security Platform アイコン」から、「Security Platform が初期化されていません」と表示されます。

2 **通知領域（Windows XP の場合）またはタスクトレイ（Windows 2000 の場合）の「Infineon Security Platform」のアイコンをクリックします。**

メニューが表示されます。

3 **「Security Platform の初期化」をクリックします。**

「Infineon Security Platform 初期化ウィザードにようこそ」が表示されます。

4 **「既存の Security Platform を復元する」にチェックをして、「次へ」をクリックします。**

「所有者権限の設定」が表示されます。

重要

- 必ず「既存の Security Platform を復元する」にチェックをしてください。

5 **所有者の「パスワード」と「パスワードの確認入力」を入力し、「次へ」をクリックします。**

「緊急時復元プロセスの設定」が表示されます。

6 **「既存の復元用アーカイブに追加する」を選択し、「参照」をクリックして緊急時復元用アーカイブの場所を指定し、「次へ」をクリックします。**

「サマリー」が表示されます。

重要

- 必ず「既存の復元用アーカイブに追加する」にチェックをしてください。「新しい復元用アーカイブを作成する」を選択すると、新しいアーカイブが以前のアーカイブに上書きされるため、以前の環境を再構築できなくなり、暗号化ファイル等を見ることができなくなります。

7 **「次へ」をクリックします。**

「緊急時復元プロセスの準備」が表示されます。

8 **「参照」をクリックし、緊急時復元用アーカイブの場所を再び指定して、「次へ」をクリックします。**

「緊急時復元用トークンの場所の指定と、パスワードの入力」が表示されます。

9 **「参照」をクリックし、緊急時復元用トークンの場所を指定し、パスワードを入力してから「次へ」をクリックします。**

「復元するコンピュータの選択」が表示されます。

10 **コンピュータを選択し、「次へ」をクリックします。**

「サマリー」が表示されます。

POINT

- 通常コンピュータは 1 台しか表示されません。

11 **「次へ」をクリックします。**

「ウィザードが正常に終了しました。」が表示されます。

12 **「完了」をクリックします。**

以上で、所有者の手順は終了します。

■ユーザ環境の再構築

POINT

- 他のアプリケーションはすべて終了してください。
- 事前にユーザーキーパスワードを確認してください。
- Trusted ログオンを設定している場合は、「一時中止パスワード」にて Windows にログオンする必要があります。

1 **Windows にログオンします。**

2 **通知領域（Windows XP の場合）またはタスクトレイ（Windows 2000 の場合）の「Infineon Security Platform」のアイコンをクリックします。**

メニューが表示されます。

3 「Security Platform の機能の復元」をクリックします。

「Security Platform ユーザー初期化ウィザードにようこそ」が表示されます。

4 「次へ」をクリックします。

「緊急時復元プロセス 基本ユーザーキーの作成または復元」が表示されます。

5 「基本ユーザーキーを復元する」にチェックをして、「次へ」をクリックします。

「緊急時復元プロセス 基本ユーザーキーの復元」が表示されます。

6 自分のユーザー名を選択し、ユーザーキーの「パスワード」を入力し、「次へ」をクリックします。

「基本ユーザーキーのパスワード設定の確認」が表示されます。

7 「次へ」をクリックします。

「Security Platform の機能の選択」が表示されます。

8 「ユーティリティの設定を行う」手順 14（→ P.17）以降の手順に従い、再設定します。

OS 入れ替え時（ハードディスク交換時）

パソコンの修理でハードディスクを交換等、OS を入れ替えた場合は、ユーザの鍵構成を再度作り直す必要がある場合があります。次の手順に従って、再構築を行ってください。

・所有者は利用者を再登録します。

・ユーザは自身の鍵を再登録し、環境を再構築します。

重要

- この操作はセキュリティチップをクリアしていないことが前提です。
- 操作を行う前に、BIOS の設定でセキュリティチップが「Enabled」（E635、E630、K630 の場合）または「使用する」（NA/H、NA/L、MG/H、MT の場合）になっていることを確認してください。（「BIOS の設定を変更する」（→ P.11））

■所有者環境の再構築

POINT

- 管理者権限でログオンしてください。
- 以下を事前に確認してください。
  ・所有者パスワード

1 「ユーティリティをインストールする」（→ P.14）の手順をすべて行います。

通知領域（Windows XP の場合）またはタスクトレイ（Windows 2000 の場合）の「Infineon Security Platform」のアイコンから、「現在のユーザー用に Security Platform が初期化されていません。」と表示されます。

2 **「スタート」ボタン→「（すべての）プログラム」→「Infineon Security Platform ツール」→「Security Platform 初期化ウィザード」の順にクリックします。**

「Infineon Security Platform 初期化ウィザードにようこそ」が表示されます。

3 **「既存の Security Platform を復元する」にチェックが入っていないことを確認し、「次へ」をクリックします。**

「管理者権限の設定」が表示されます。

4 **所有者の「パスワード」を入力し、「次へ」をクリックします。**

「緊急時復元プロセスの設定」が表示されます。

5 **「新しい復元用アーカイブを作成する」をチェックして、保存場所を確認し、「次へ」をクリックします。**

「Security Platform の緊急時復元用トークンのパスワード入力」が表示されます。

重要

- 緊急時復元用アーカイブの保存場所は通常、表示されている場所から変更する必要はありません。

6 **緊急時復元用トークンの「パスワード」と「パスワードの確認入力」に入力し、「次へ」をクリックします。**

「復元用トークンの保存」が表示されます。

7 **緊急時復元用トークンの保存場所を設定し、「次へ」をクリックします。**

「サマリー」が表示されます。

重要

- 保存先は仮の場所が表示されています。緊急時復元用トークンは、リムーバブルドライブ等、パソコン本体とは別の場所に保管できる媒体に保存することをお勧めします。

8 **「次へ」をクリックします。**

しばらくすると、「ウィザードが正常に終了しました。」が表示されます。

9 **「完了」をクリックします。**

■ユーザ環境の再構築

POINT

- 以下を事前に確認してください。
  - ・バックアップファイル
  - ・ユーザーキーパスワード

1 **Windows にログオンします。**

2 **「スタート」ボタン→「（すべての）プログラム」→「Infineon　Secure Platform ツール」→「Security Platform バックアップツール」の順にクリックします。**

「Infineon Security Platform のバックアップ／復元ウィザードにようこそ」が表示されます。

3 **「次へ」をクリックします。**

「バックアップまたは復元」が表示されます。

4 **「キーと証明書の復元」をチェックして、「次へ」をクリックします。**

「設定を復元する」が表示されます。

5 **「参照」をクリックし、復元するファイルの場所を指定し、「次へ」をクリックします。**

「サマリー」が表示されます。

6 **「次へ」をクリックします。**

「ウィザードが正常に終了しました。」が表示されます。

7 **「Security　Platform 初期化ウィザードを起動する」にチェックをして、「完了」をクリックします。**

「Security Platform の機能」が表示されます。

8 **「電子メールの保護」と「ファイルとフォルダの暗号化（EFS）」にチェックをして、「次へ」をクリックします。**

9 **「次へ」をクリックします。**

「暗号化証明書」が表示されます。

10 **「選択」ボタンをクリックして、自分のユーザー名を選択します。**

「設定の確認」が表示されます。

11 **「次へ」をクリックします。**

「ウィザードが正常に終了しました。」が表示されます。

12 **「完了」をクリックします。**

13 **「ユーザーキーパスワード」を変更してください。**

ユーザーキーパスワードを入力することで、所有者に鍵構成の再構築完了を通知します。「パスワードの変更」（→ P.23）を参照してください。

パソコン廃却時のセキュリティチップへの設定

パソコンを廃却する際には、パソコンに残ったデータを復元できないようにすることが重要です。セキュリティチップにより保護されたデータは、セキュリティチップ内のデータを破棄し、復元用ファイルを破棄することで再び復元することができなくなります。これは、BIOS にてセキュリティチップを「クリア」し、また、緊急時復元用トークンを破棄することで、データを復旧することができなくなります。

・「E635 の場合」(→ P.35)

・「E630、K630 の場合」(→ P.36)

・「NA/H、NA/L、MG/H、MT の場合」(→ P.36)

重要

- この操作はセキュリティチップのデータを破棄するだけで、ハードディスクのデータは破棄されません。セキュリティチップのデータを破棄したことで、ハードディスク内のセキュリティチップの保護されたデータは見ることができなくなりますが、実際の廃却時にはハードディスクのデータをクリアしてください。
- BIOS の設定で、セキュリティチップ関連の設定を行うには、管理者用パスワードを設定する必要があります。
- BIOS セットアップについて詳しくは、パソコン本体の『FMV マニュアル』の「BIOS」を参照してください。

■ E635 の場合

1 **「4　インストールを行う」－「BIOS の設定を変更する」－「E635 の場合」(→ P.11) の手順 1 ～ 6 を行います。**

2 **【↑】キーまたは【↓】キーを押して、「Clear Security Chip」を選択し、【Enter】キーを押します。**

クリアを続行してよいかを確認するウィンドウが表示されます。

3 **「Ok」を選択し、【Enter】キーを押します。**

4 **Exit メニューが表示されるまで、何度か【Esc】キーを押します。**

5 **【↑】キーまたは【↓】キーを押して「Exit Saving Changes」を選択し、【Enter】キーを押します。**

「Save Configuration Changes and exit now?」が表示されます。

6 **【←】キーまたは【→】キーを押して「Ok」を選択し、【Enter】キーを押します。**

BIOS セットアップが終了し、パソコン本体が再起動します。

7 **緊急時復元用トークンを削除します。**

重要

- セキュリティチップの設定を有効にするには、BIOS セットアップ終了後にパソコン本体の再起動が必要です。

■ E630、K630 の場合

1 **「4　インストールを行う」－「BIOS の設定を変更する」－「E630、K630 の場合」（→ P.12）の手順 1 ～ 7 を行います。**

2 **【↑】キーまたは【↓】キーを押して、「Clear Security Chip」を選択し、【Enter】キーを押します。**

クリアを続行してよいかを確認するウィンドウが表示されます。

3 **「Yes」を選択し、【Enter】キーを押します。**

4 **Exit メニューが表示されるまで、何度か【Esc】キーを押します。**

5 **【↑】キーまたは【↓】キーを押して「Exit Saving Changes」を選択し、【Enter】キーを押します。**

「Save Configuration Changes and exit now?」が表示されます。

6 **【←】キーまたは【→】キーを押して「Yes」を選択し、【Enter】キーを押します。**

BIOS セットアップが終了し、パソコン本体が再起動します。

7 **緊急時復元用トークンを削除します。**

重要

- 「セキュリティチップ」の設定を有効にするには、BIOS セットアップ終了後にパソコン本体の再起動が必要です。終了メニューで「Exit Saving Changes」を行っただけで電源を切ってしまうと、設定が正しく行われませんのでご注意ください（次回起動時にエラーメッセージが表示されます）。

■ NA/H、NA/L、MG/H、MT の場合

1 **「4　インストールを行う」－「BIOS の設定を変更する」－「NA/H、NA/L、MG/H、MT の場合」（→ P.13）の手順 1 ～ 7 を行います。**

2 **【↑】キーまたは【↓】キーを押して、「セキュリティチップのクリア」を選択し、【Enter】キーを押します。**

クリアを続行してよいかを確認するウィンドウが表示されます。

3 **「はい」を選択し、【Enter】キーを押します。**

4 **【↑】キーまたは【↓】キーを押して、「セキュリティチップ」を選択します。**

5 **【Space】キーまたは【－】キーを押して、「使用しない」を選択します。**

6 **終了メニューが表示されるまで、何度か【Esc】キーを押します。**

7 **【↑】キーまたは【↓】キーを押して「変更を保存して終了する」を選択し、【Enter】キーを押します。**

「セットアップ確認」が表示されます。

8 **【←】キーまたは【→】キーを押して「はい」を選択し、【Enter】キーを押します。**

BIOS セットアップが終了し、パソコン本体が再起動します。

9 **緊急時復元用トークンを削除します。**

重要

- 「セキュリティチップ」の設定を有効にするには、BIOS セットアップ終了後にパソコン本体の再起動が必要です。終了メニューで「変更を保存する」を行っただけで電源を切ってしまうと、設定が正しく行われませんのでご注意ください（次回起動時にエラーメッセージが表示されます）。

7 トラブルシューティング

□ BIOS でセキュリティチップの設定を変更できない

BIOS で、セキュリティチップを使用するかどうかや、セキュリティチップのデータをクリアする設定を行うためには、管理者用パスワードの設定が必要です。管理者用パスワードが設定されているか確認してください。

□ Infineon Security Platform がインストールできない

Infineon Security Platform をインストールするには、BIOS でセキュリティチップを使用する設定になっている必要があります。BIOS の設定を確認してください。

□ SMARTACCESS/Trust が起動できない

SMARTACCESS/Trust を起動するには、Infineon Security Platform が正常にインストールされ、初期化ウィザードとユーザー初期化ウィザードが正常に終了している必要があります。確認してください。

□ Trusted ログオン時に機器が変更された旨のエラーメッセージが表示される

前回の起動からハードウェアの構成や設定が変更された可能性があります。ハードウェア構成や BIOS 設定など変更されていないか確認してください。変更があった場合は、機器を登録したときの状態に戻してください。

□ Trusted ログオン時にパスワードエラーになる

Trusted ログオンを有効にしている場合には、Windows のパスワードではなくセキュリティチップのユーザーキーパスワードを入力してください。

□ EFS が利用できない

EFS を利用するにはハードディスクが NTFS でフォーマットされていることが必要です。FAT32 のドライブでは EFS を利用することはできません。NTFS に変換するにはパソコン本体の『FMV マニュアル』の「機能」を参照してください。なお、Windows XP Home Edition では、EFS は利用できません。

□ ダイヤルアップにアプリケーションログオンを行うとパスワードが見える

Windows に標準で添付されるダイヤルアップの ID・パスワード入力を、SMARTACCESS/Trust のアプリログオン機能を使って自動入力を行うと、パスワードが隠し文字とならず、読めてしまう場合があります。この場合は、ダイヤルアップの画面にて「次のユーザが接続するとき使用するために、このユーザー名とパスワードを保存する」のチェックを外してください。パスワードも隠し文字とすることができます。

□ セキュリティチップを「Disabled」（E635、E630、K630 の場合）または「使用しない」（NA/H、NA/L、MG/H、MT の場合）に設定すると、Windows にログオンできなくなった

Trusted ログオンを設定した状態で、セキュリティチップを「Disabled」（E635、E630、K630 の場合）または「使用しない」（NA/H、NA/L、MG/H、MT の場合）に設定すると、セキュリティチップにて保存していた Windows パスワードが利用できないため、Windows にログオンできなくなります。その際にはセキュリティチップを「Enabled」（E635、E630、K630 の場合）または「使用する」（NA/H、NA/L、MG/H、MT の場合）にし直すか、「一時中止パスワード」にてログオンする必要があります。なお、「一時中止パスワード」にてログオンしても、セキュリティチップにて保護された環境は安全に管理されています。

□ ハードウェア構成を変更したために Windows にログオンできなくなった

ハードウェアの構成を変更すると、SMARTACCESS/Trust の機器監査機能により Windows にログオンできなくなります。その際にはハードウェア構成を登録したときの設定に戻すか、機器構成を登録しなおす必要があります。詳しい設定方法については、SMARTACCESS/Trust のマニュアルの「3.5 ログオンする」を参照してください。

□ Trusted ログオンでパスワードの入力画面が 2 度表示される

「ユーザーキーパスワード」と「一時中止パスワード」を同じにしている可能性があります。管理者にご相談ください。

□ Trusted ログオン時、内部エラー (0xe0280012) が表示される

セキュリティチップがクリアされた可能性があります。管理者にご相談ください。

□「OS 入れ替え時」の作業完了後、ユーザーキーパスワードが以前のパスワードに戻る

「Security Platform のバックアップ／復元ウィザード」にてユーザーキーを復元すると、バックアップを取ったときのパスワードに戻ります。

□ Windows 2000 でユーザがファイルを暗号化した場合、Administrator から暗号化ファイルが読める

ファイル暗号は、Windows 標準の EFS の機能を使って行っています。Windows 2000 では EFS 暗号化を行うと、Administrator からユーザの暗号化ファイルを読むことができます。これは Windows 2000 の「回復エージェント」が Administrator になっているためです。詳しくは、Windows 2000 のマニュアルを参照してください。なお、Windows XP では、「回復エージェント」が Administrator に指定されていないため、ユーザの暗号化ファイルを読むことはできません。

FMV シリーズ
セキュリティチップ
取扱説明書

B6FH-4341-01　Z2-01

発 行 日　2004 年 10 月
発行責任　富士通株式会社